AMENDMENTS TO THE CLAIMS

1-28 (Canceled).

29. (Currently Amended) A method comprising:

for each electronic device of a plurality of electronic devices, in real time:

on the electronic device, at a transport layer, capturing substantially all digital data ~~sent from a network to~~ received by the electronic device over a network before the digital data is provided to an application layer for presentation to a user of the electronic device;

transmitting information related to the captured digital data to a backend system on the network, the backend system comprising at least one server;

delaying delivery of the digital data to the application layer on the electronic device at least until the digital data is designated non-illicit by ~~a backend system on the network, the backend system comprising~~ the at least one server, the at least one server providing a content-rating service ~~for rating~~ that rates illicitness of digital data;

receiving an indication from the at least one server of whether the captured digital data is illicit digital data or non-illicit digital data, the indication resulting at least in part from the content-rating service; and

blocking the illicit digital data from delivery to the application layer.

30. (Previously Presented) The method of claim 29, comprising, for each of the plurality of electronic devices, in real time, allowing delivery of the non-illicit digital data to the application layer for presentation to the user of the electronic device.

31. (Previously Presented) The method of claim 29, comprising, for each of the plurality of electronic devices, in real time, capturing substantially all requests for digital data over the network by the electronic device.

32. (Previously Presented) The method of claim 31, comprising:

for each of the plurality of electronic devices, concurrently routing:

information relating to at least some of the captured requests for digital data to the at least one server providing the content-rating service; and

the at least some captured requests to intended destinations on the network.

33. (Previously Presented) The method of claim 32, wherein at least some of the captured digital data is digital data received at the electronic device as a result of the step of routing the information relating to at least some of the captured requests for digital data to the intended destinations.

34. (Previously Presented) The method of claim 32, wherein at least some of the captured digital data is digital data received at the electronic device independent of the routing step.

35. (Currently Amended) The method of claim 32, comprising, on the at least one server: [[,]]

crawling the digital data on the network using the at least some of the captured requests; and

rating the digital data for illicitness using a word-by-word analysis of the digital data.

36. (Previously Presented) The method of claim 35, further comprising, responsive to the rating step, storing a rating and identification information for the rated digital data together in a content database in communication with the at least one server.

37. (Previously Presented) The method of claim 29, comprising, for each of the plurality of electronic devices, sending an authentication signal to the backend system, the authentication signal providing validation information indicating whether the electronic device corresponds to a valid user account.

38. (Previously Presented) The method of claim 29, further comprising, for each of the plurality of electronic devices, filtering communication between the electronic device and the network for personal information.

39. (Previously Presented) The method of claim 29, further comprising, for each of the plurality of electronic devices, filtering communication between the electronic device and the network for explicit requests for illicit content.

40. (Previously Presented) The method of claim 29, wherein the electronic device comprises at least one of:

a personal computer;
a set-top box;
a router; and
a gateway.

41. (Previously Presented) The method of claim 35, further comprising transmitting configuration settings to the electronic device corresponding to the valid user account.

42. (Previously Presented) The method of claim 29, wherein at least some of the digital data comprises an instant message en route to an instant messaging application on the electronic device.

43. (Previously Presented) The method of claim 29, wherein at least some of the digital data comprises an email message en route to an email application on the electronic device.

44. (Previously Presented) The method of claim 29, further comprising, for at least one of the electronic devices, rating the digital data for illicitness utilizing a content-rating module on the electronic device.

45. (Previously Presented) The method of claim 29, comprising, for at least one of the plurality of electronic devices:

transmitting information related to the captured digital data to a reporting server; and

on the reporting server, logging network activities of the user of the electronic device via the information related to the captured digital data.

46. (Previously Presented) The method of claim 45, comprising:

on the reporting server, for the at least one of the plurality of electronic devices:

generating a report summarizing illicitness of network activities of the user of the electronic device for a predetermined time period; and

transmitting the report over the network to a third party.

47. (Previously Presented) The method of claim 45, comprising:

wherein the at least one of the plurality of electronic devices comprises more than one electronic device;

generating a multi-user report summarizing illicitness of network activities of each user of the more than one electronic device for a predetermined time period; and

transmitting the multi-user report over the network to a third party.

48. (Previously Presented) The method of claim 29, comprising, for at least one of the plurality of electronic devices:

delaying delivery of the digital data to the application layer on the electronic device at least until the digital data is designated non-malicious by the backend system;

receiving an indication from the backend system on whether the digital data is malicious or non-malicious; and

blocking the digital data deemed to be malicious.

49. (Previously Presented) The method of claim 31, comprising, for at least one of the plurality of electronic devices:

receiving an indication from the backend system that at least one of the captured requests for digital data represents an unauthorized intrusion on the electronic device; and

denying the at least one of the captured requests for digital data.

50. (Previously Presented) A method comprising:

capturing, on an electronic device, substantially all requests for digital content over a network;

on the electronic device, concurrently routing:

information relating to at least some of the captured requests for digital content to a backend system on the network, the backend system having at least one server providing a content-rating service; and

the at least some captured requests to intended destinations on the network;

on the at least one server on the backend system, rating the digital content being requested in the at least some of the requests for digital content using the content-rating service;

receiving, on the electronic device, an indication from the at least one server of illicit or non-illicit for each of the at least some requests for digital content, the indication being at least partially based on the rating step; and

restricting presentation of any digital content for which the illicit indication is received to a user of the electronic device.

51. (New) A method comprising:

for each electronic device of a plurality of electronic devices, in real time:

on the electronic device, at a transport layer, capturing substantially all digital data received by the electronic device over a network before the digital data is provided to an application layer for presentation to a user of the electronic device;

routing information related to the digital data to a backend system on the network, the backend system comprising at least one server, the at least one server providing a content-rating service for rating digital-data illicitness;

delaying delivery of the digital data to the application layer on the electronic device at least until the digital data is designated non-illicit by the at least one server;

on the at least one server, determining a digital-data rating via the information related to the digital data, the determining comprising:

checking a ratings database for a pre-existing rating for the digital data using an address included in the information related to the digital data;

responsive to the address being found in the ratings database, using the pre-existing rating as the digital-data rating;

responsive to the digital data not being found in the ratings database:

crawling the digital data via the address;

accessing the digital data over the network;

performing a word-by-word analysis of the digital data to determine the digital-data rating; and

updating the ratings database with the address and the digital-data rating responsive to the performance of the word-by-word analysis;

designating the digital data as illicit digital data or non-illicit digital data, the designating comprising designating the digital data as illicit digital data if the digital-data rating exceeds a predetermined threshold;

on the electronic device, receiving the designation from the at least one server; and

on the electronic device, blocking the illicit digital data from delivery to the application layer.